

What is claimed is:

- 1     1.     A method comprising:
  - 2             performing an authentication of a computing device and equipment of an
  - 3             operator of services for the computing device for a session of communication
  - 4             between the computing device and the equipment, the performing comprising:
    - 5                 generating, in the computing device, a random number;
    - 6                 generating a one-time-pad key based on a hash operation of a value
    - 7                 selected from the group consisting of an identification of the computing device, an
    - 8                 identification of the equipment, a platform configuration measurement of the
    - 9                 computing device stored in a protected storage within the computing device and an
    - 10                identification of the session of communication stored in the protected storage within
    - 11                the computing device;
    - 12                encrypting the random number based on the one-time-pad key;
    - 13                transmitting the encrypted random number to the equipment;
    - 14                receiving, from the equipment, an encrypted value in response to the
    - 15                encrypted random number, wherein the encrypted value includes a challenge of a
    - 16                challenge-response;
    - 17                verifying the encrypted value;
    - 18                encrypting a response to the challenge of the challenge-response;
    - 19                transmitting the response to the equipment; and
    - 20                receiving, from the equipment, an authentication verification.
- 1     2.     The method of claim 1, wherein the platform configuration measurement of
- 2             the computing device comprises a version of hardware in the computing device.
- 1     3.     The method of claim 1, wherein the platform configuration measurement of
- 2             the computing device comprises a version of software executing in the computing
- 3             device.

1 4. The method of claim 1, wherein the challenge of the challenge-response  
2 comprises an encryption of a data string that includes a concatenation of the random  
3 number generated in the computing device, a random number generated by the  
4 equipment and the identification of the session.

1 5. The method of claim 4, wherein the response of the challenge-response  
2 comprises an encryption of a data string that includes a concatenation of the random  
3 number generated in the computing device and the random number generated by the  
4 equipment.

1 6. The method of claim 1, further comprising auditing the authentication,  
2 wherein auditing comprises:  
3 storing at least one attribute of the authentication into an audit log within a  
4 memory of the computing device;  
5 encrypting the audit log based on an encryption key that is generated and  
6 stored within the computing device;  
7 generating an integrity metric of the audit log; and  
8 generating a signature of the integrity metric with a signature key that is  
9 generated and stored within the computing device.

1 7. The method of claim 6, wherein auditing the authentication further  
2 comprises generating a signature of a value of an audit counter with the signature  
3 key.

1 8. A method comprising:  
2 authenticating a computing device and a different entity for a session of  
3 communication between the computing device and the different entity, the  
4 authenticating comprising:  
5 generating a hash of a value selected from the group consisting of a  
6 platform configuration value associated with computing device stored in the

7 computing device and the identification of the session stored in a protected storage  
8 within the computing device and;  
9 encrypting a random number based on the hash; and  
10 transmitting the encrypted random number to the different entity.

1 9. The method of claim 8, wherein the authenticating further comprises:  
2 encrypting a response to a challenge of a challenge-response, wherein the  
3 challenge is received, in response to the encrypted random number, as part of an  
4 encrypted value from the different entity; and  
5 transmitting the encrypted response to the different entity.

1 10. The method of claim 8, further comprising commencing a transaction  
2 between the computing device and the different entity, after receiving an  
3 authentication verification message in response to the encrypted response from the  
4 different entity.

1 11. The method of claim 8, further comprising auditing the authenticating,  
2 wherein auditing comprises:  
3 storing at least one attribute of the authenticating into an audit log within a  
4 memory of the computing device;  
5 encrypting the audit log based on an encryption key that is generated and  
6 stored within the computing device;  
7 generating an integrity metric of the audit log; and  
8 generating a signature of the integrity metric with a signature key that is  
9 generated and stored within the computing device.

1 12. The method of claim 11, wherein auditing the authenticating further  
2 comprises generating a signature of a value of an audit counter with the signature  
3 key.

1 13. The method of claim 12, wherein auditing the authenticating further  
2 comprises appending the integrity metric, the signature of the integrity metric, the  
3 signature of the value of the audit counter and the value of the audit counter to the  
4 audit log.

1  
2 14. The method of claim 8, wherein the platform configuration value associated  
3 with the computing device comprises a version of hardware in the computing  
4 device.

1 15. The method of claim 8, wherein the platform configuration value associated  
2 with the computing device comprises a version of software executing in the  
3 computing device.

1 16. A method comprising:  
2 authenticating a computing device and equipment of a provider of services  
3 for the computing device for a session of communication between the computing  
4 device and the equipment, the authenticating comprising:  
5 receiving a number that is encrypted with a hash of a value selected  
6 from the group consisting of a platform configuration value associated with  
7 computing device stored in the computing device and the identification of the  
8 session;  
9 recovering the number; and  
10 encrypting, in response to receiving the hash, a value from the group  
11 consisting of a challenge of a challenge-response that includes the number, a  
12 random number generated in the equipment and an attestation key; and  
13 transmitting the encrypted value to the computing device.

1 17. The method of claim 16, wherein authenticating further comprises  
2 generating the challenge of the challenge-response, wherein generating of the  
3 challenge comprises encrypting, using the session key, from values selected from

4 the group consisting of the number from the computing device, the random number  
5 generated in the equipment and a different identification of the session.

1 18. The method of claim 16, wherein authenticating further comprises:  
2 receiving a response of the challenge-response, wherein the response is  
3 encrypted;  
4 decrypting the response that is encrypted; and  
5 verifying that the response includes values selected from the group  
6 consisting of the number from the computing device and the random number  
7 generated in the equipment.

1 19. The method of claim 16, wherein the platform configuration value  
2 associated with the computing device comprises a version of hardware in the  
3 computing device.

1 20. The method of claim 16, wherein the platform configuration value  
2 associated with the computing device comprises a version of software executing in  
3 the computing device.

1 21. A system comprising:  
2 a Synchronous RAM (SRAM) to store at least a part of a number of  
3 instructions to cause authentication of the system to equipment of a provider of  
4 services for the system and to cause authentication of the equipment to the system;  
5 a processor to execute the number of instructions;  
6 a cryptographic processing module comprising:  
7 at least one storage register to store an encrypted configuration  
8 associated with the system and an identification of a session of communication  
9 between the system and the equipment of the provider of services for the system;  
10 a random number generation logic to generate a random number;  
11 a hashing logic to generate, based on the execution of the number of  
12 instructions, a hash of a value selected from the group consisting of the encrypted

13 configuration associated with the system and the identification of the session of  
14 communication; and  
15 an encryption logic to encrypt the random number based on hash;  
16 an input/output (I/O) logic to transmit the random number to the equipment  
17 of the provider of services for the system.

1 22. The system of claim 21, wherein the I/O logic is to receive an encrypted  
2 message from the equipment, in response to the random number, wherein the  
3 encrypted message includes values from the group consisting of a challenge of a  
4 challenge-response, a random number generated in the equipment and an attestation  
5 key.

1 23. The system of claim 21, wherein the encryption logic is to encrypt a  
2 response to the challenge of the challenge-response, wherein the I/O logic is to  
3 transmit the encrypted response to the equipment of the provider of services for the  
4 system.

1 24. The system of claim 23, wherein the I/O logic is to transmit a  
2 communication with an entity on a network to which the equipment is coupled after  
3 receipt of an authentication message from the equipment in response to the  
4 encrypted response.

1 25. A machine-readable medium that provides instructions, which when  
2 executed by a machine, cause said machine to perform operations comprising:  
3 performing an authentication of a computing device and equipment of an  
4 operator of services for the computing device for a session of communication  
5 between the computing device and the equipment, the performing comprising:  
6 generating, in the computing device, a random number;  
7 generating a one-time-pad key based on a hash operation of a value  
8 selected from the group consisting of an identification of the computing device, an

9 identification of the equipment, a platform configuration measurement of the  
10 computing device stored in a protected storage within the computing device and an  
11 identification of the session of communication stored in the protected storage within  
12 the computing device;  
13                 encrypting the random number based on the one-time-pad key;  
14                 transmitting the encrypted random number to the equipment;  
15                 receiving, from the equipment, an encrypted value in response to the  
16 encrypted random number, wherein the encrypted value includes a challenge of a  
17 challenge-response;  
18                 verifying the encrypted value;  
19                 encrypting a response to the challenge of the challenge-response;  
20                 transmitting the response to the equipment; and  
21                 receiving, from the equipment, an authentication verification.

1 26. The machine-readable medium of claim 25, wherein the challenge of the  
2 challenge-response comprises an encryption of a data string that includes a  
3 concatenation of the random number generated in the computing device, a random  
4 number generated by the equipment and the identification of the session.

1 27. The machine-readable medium of claim 26, wherein the response of the  
2 challenge-response comprises an encryption of a data string that includes a  
3 concatenation of the random number generated in the computing device and the  
4 random number generated by the equipment.

28. A machine-readable medium that provides instructions, which when  
executed by a machine, cause said machine to perform operations comprising:  
1                 authenticating a computing device and a different entity for a session of  
2 communication between the computing device and the different entity, the  
3 authenticating comprising:  
4                 generating a hash of a value selected from the group consisting of a  
5 platform configuration value associated with computing device stored in the

6 computing device and the identification of the session stored in a protected storage  
7 within the computing device;

8 encrypting a random number based on the hash; and  
9 transmitting the encrypted random number to the different entity.

1 29. The machine-readable medium of claim 28, wherein the authenticating  
2 further comprises:

3 encrypting a response to a challenge of a challenge-response, wherein the  
4 challenge is received, in response to the encrypted random number, as part of an  
5 encrypted value from the different entity; and

6 transmitting the encrypted response to the different entity.

1 30. The machine-readable medium of claim 28, further comprising commencing  
2 a transaction between the computing device and the different entity, after receiving  
3 an authentication verification message in response to the encrypted response from  
4 the different entity.

1 31. A machine-readable medium that provides instructions, which when  
2 executed by a machine, cause said machine to perform operations comprising:  
3 authenticating a computing device and equipment of a provider of services  
4 for the computing device for a session of communication between the computing  
5 device and the equipment, the authenticating comprising:

6 receiving a number that is encrypted with a hash of a value selected  
7 from the group consisting of a platform configuration value associated with  
8 computing device stored in the computing device and the identification of the  
9 session;

10 recovering the number;

11 encrypting, in response to receiving the hash, a value from the group  
12 consisting of a challenge of a challenge-response that includes the number, a  
13 random number generated in the equipment and an attestation key; and

14 transmitting the encrypted value to the computing device.



1 32. The machine-readable medium of claim 31, wherein authenticating further  
2 comprises generating the challenge of the challenge-response, wherein generating of  
3 the challenge comprises encrypting, using the session key, from values selected  
4 from the group consisting of the number from the computing device, the random  
5 number generated in the equipment and a different identification of the session.

1 33. The machine-readable medium of claim 31, wherein authenticating further  
2 comprises:

3 receiving a response of the challenge-response, wherein the response is  
4 encrypted;

5 decrypting the response that is encrypted; and

6 verifying that the response includes values selected from the group  
7 consisting of the number from the computing device and the random number  
8 generated in the equipment.